LISTING OF THE CLAIMS:

This listing of claims replaces all prior versions, and listings, of claims in the application:

- 1-21. (Canceled)
- 1 22. (Previously Presented) An apparatus for producing a pseudo random sequence, comprising:
- a data bit generator to produce a principal data stream;
- 3 multiple data bit generators to create additional data streams;
- 4 a storage structure responsive to the additional data streams having multiple bit storage
- 5 locations to store the bits of the principal data stream in the storage locations in a pseudo random
- 6 order based on an order of bits in the additional data streams; and
- a shuffle unit coupled with the data bit generators to modify the principal data stream by
- 8 combining the bits of the principal data stream with past bits of the principal data stream stored
- 9 in the storage structure and pseudo randomly selected from the storage structure based on an
- order of the bits in the additional data streams to produce a pseudo random sequence.
- 1 23. (Previously Presented) An apparatus according to claim 22, wherein the data bit generators
- 2 comprise linear feedback shift registers.
- 1 24. (Previously Presented) An apparatus according to claim 22, wherein the storage unit has a
- 2 number of addressable bit locations and wherein the additional data streams control write address
- 3 and read address ports that control access to the number of addressable bit locations.
- 1 25. (Previously Presented) An apparatus according to claim 24, wherein the number of
- 2 addressable bit locations is a number that has a base 2 relationship with the number of multiple
- 3 data bit generators.

1 26. (Previously Presented) An apparatus according to claim 22, wherein the shuffle unit includes

- 2 a 1 to n (n an integer greater than 1) de-multiplexer having an input line coupled to the data bit
- 3 generator that produces the principal data stream, control lines, at least one of which is coupled
- 4 to one of the multiple data bit generators, and n output lines coupled to the storage structure.
- 1 27. (Previously Presented) An apparatus according to claim 22, wherein the shuffle unit includes
- 2 an n to 1 (n an integer greater than 1) multiplexer having n input lines coupled to the storage
- 3 structure, an output line, and control lines, at least one of which is coupled to one of the multiple
- 4 data bit generators.
- 1 28. (Previously Presented), An apparatus according to claim 22, wherein the shuffle unit further
- 2 includes a bit-wise XOR circuit, an input of which receives the bits of the principal data stream
- 3 and an input of which receives the pseudo randomly selected bits, the output of which is the
- 4 pseudo random sequence..
- 1 29. (Previously Presented) A method for generating a data stream, comprising:
- 2 generating a first and a second bit sequence;
- 3 storing bits from the first sequence in a memory structure;
- 4 retrieving stored bits of the first sequence from the memory structure in a stochastic
- 5 order, the order based at least in part on a bit order of the second sequence;
- bit-wise modifying the bits of the first sequence with the stochastically retrieved bits to
- 7 produce a pseudo random data stream.

- 1 30. (Previously Presented) A method according to claim 29, wherein generating the first and
- 2 second bit sequences comprises generating at least one of the first and the second bit sequences
- 3 with a linear feedback shift register.
- 1 31. (Previously Presented) A method according to claim 29, wherein storing bits from the first
- 2 sequence in a memory structure comprises writing to bit-addressable memory locations in the
- 3 memory structure an address selected output of a 1 to n (n being an integer greater than 1) de-
- 4 multiplexer, the input of the multiplexer being the first bit sequence, and the address selection
- 5 controlled by an order of bits in the second bit sequence.
- 1 32. (Previously Presented) A method according to claim 29, wherein retrieving stored bits in the
- 2 stochastic order from the memory structure comprises retrieving an output of an n to 1 (n being
- an integer greater than 1) multiplexer, the n address selectable inputs of the multiplexer
- 4 corresponding to n bit-addressable memory locations in the memory structure, and the address
- 5 selection controlled by an order of bits in the second bit sequence.
- 1 33. (Previously Presented) A method according to claim 29, wherein bit-wise modifying the bits
- 2 of the first sequence comprises logically XOR-ing the bits of the first bit sequence with the
- 3 stochastically retrieved bits.
- 1 34. (Previously Presented) A method according to claim 29, further comprising generating
- 2 additional bit sequences, wherein storing and retrieving bits to/from the memory structure

- 3 comprise storing and retrieving in a stochastic order based on a combined bit order of the second
- 4 and the additional bit sequences.
- 1 35. (Previously Presented) A stream cipher generator comprising:
- 2 a first data bit generator to produce a first stream of data bits;
- a memory having a read and write port to receive and store bits from the first stream of
- 4 data bits;
- 5 a second data bit generator to produce a second stream of data bits;
- a read and write port controller coupled to the memory and responsive to the second
- 7 stream of data bits, to control the read and write functions of the memory based, at least in part,
- 8 on the sequence of bits in the second stream of data bits; and
- a combiner to receive the first stream of data bits and the bits read from the memory, and
- modify the first stream of data bits with the bits read from the memory to produce a pseudo
- 11 random sequence.
- 1 36. (Previously Presented) A stream cipher generator according to claim 35, wherein at least one
- 2 of the first and the second data bit generators comprise a linear feedback shift register.
- 1 37. (Previously Presented) A stream cipher generator according to claim 35, wherein the
- 2 memory further includes a bit-addressable address selection port.
- 1 38. (Previously Presented) A stream cipher generator according to claim 37, wherein the read
- 2 and write port controller further comprises a 1 to n (n being an integer greater than 1) de-

3 multiplexer, the de-multiplexer input coupled to the first data bit generator, the n outputs coupled

- 4 to n bit locations of the bit-addressable memory, and a control line coupled to the second data bit
- 5 generator to make the address selection responsive to an order of bits in the second stream of
- 6 data bits.
- 1 39. (Previously Presented) A stream cipher generator according to claim 37, wherein the read
- 2 and write port controller further comprises an n to 1 (n being an integer greater than 1)
- 3 multiplexer, the n multiplexer inputs coupled to n locations of the bit-addressable memory, the
- 4 multiplexer output coupled to the combiner, and a control line coupled to the second data bit
- 5 generator to make the address selection responsive to an order of bits in the second stream of
- 6 data bits.
- 1 40. (Previously Presented) A stream cipher generator according to claim 37, further comprising
- 2 additional data bit generators, and wherein the read and write port controller controls the read
- 3 and write functions of the memory based on a sequence of bits of the combination of the second
- 4 stream of data bits and data streams generated by the additional data bit generators.
- 1 41. (Previously Presented) A stream cipher generator according to claim 35, wherein the
- 2 combiner comprises a bit-wise XOR circuit to XOR the bits of the first stream of data bits with
- 3 the bits read from the memory, and the XOR output comprises the pseudo random sequence.